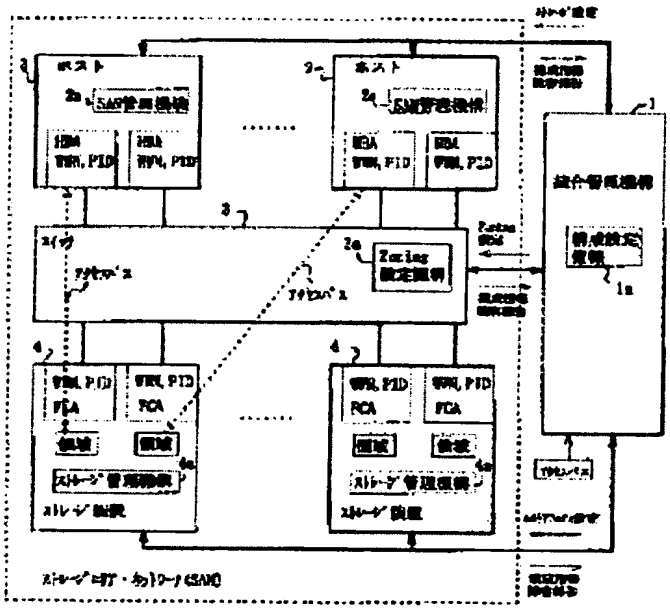
STORAGE AREA NETWORK MANAGING SYSTEM

Patent number: JP2002063063
Publication date: 2002-02-28
Inventor: IWATANI SAWAO
Applicant: FUJITSU LTD
Classification:
- international: G06F12/00; G06F12/14
- european:
Application number: JP20010167946 20010604
Priority number(s): JP20010167946 20010604; JP20000167482 20000605

Abstract of **JP2002063063**

PROBLEM TO BE SOLVED: To automatically perform best security management for a SAN (storage area network) by unitarily integrating/managing conventional discrete security methods. SOLUTION: An integrating/managing mechanism 1 for integrating/managing SAN is installed, so that access relations between hosts 2 and storage devices 4 can be collectively managed by using the managing mechanism 1. Access paths, that is, areas on the storage device 4 side which are to be accessed from the host 2 side, and fiber channel adaptors(FCAs) and host bus adaptors(HBAs), which are used when the storages are accessed, are set in the mechanism 1. Based on access path information set, the mechanism 1 performs storage settings, a zoning setting, and settings for which area to permit access, for SAN managing mechanism 2a of the hosts 2, a zoning setting mechanism 3a of a switch 3, and storage managing mechanisms 4a of the storage devices 4, respectively.

本発明の概要を説明する図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－63063
（P2002－63063A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	12/00	５４５	Ｇ０６Ｆ　12/00	５４５Ｂ	５Ｂ０１７
		５３７		５３７Ａ	５Ｂ０８２
	12/14	３２０	12/14	３２０Ａ	

審査請求　未請求　請求項の数９　ＯＬ　（全 20 頁）

(21)出願番号　特願2001－167946(P2001－167946)
(22)出願日　平成13年６月４日(2001.6.4)
(31)優先権主張番号　特願2000－167482(P2000－167482)
(32)優先日　平成12年６月５日(2000.6.5)
(33)優先権主張国　日本（ＪＰ）

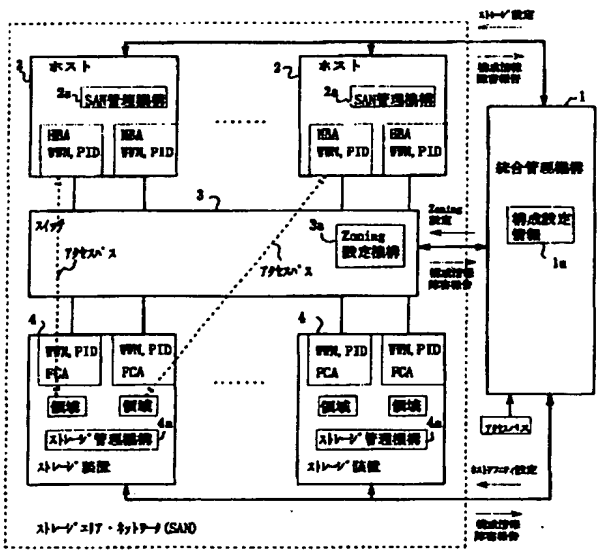
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岩谷　沢男
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100100930
弁理士　長澤　俊一郎　（外１名）

Ｆターム(参考)　5B017 AA03 BA06 CA07
5B082 EA11

(54)【発明の名称】　ストレージエリア・ネットワーク管理システム

(57)【要約】
【課題】　従来の分割されたセキュリティ方式を一元的に統合管理し、ＳＡＮにおいて最善のセキュリティ管理を自動的に行うこと。
【解決手段】　ＳＡＮを統合制御する統合管理機構１を設置し、ホスト２とストレージ装置４とのアクセス関係をこの管理機構１を用いて一括して管理できるようにする。統合管理機構１にアクセスパス、すなわち、ホスト２側からアクセスをしようとするストレージ装置４側の領域と、そのストレージをアクセスする際の使用するファイバチャネルアダプタ（ＦＣＡ）、ホストバスアダプタ（ＨＢＡ）を設定する。設定されたアクセスパス情報を元に、統合管理機構１は、ホスト２のＳＡＮ管理機構２ａ、スイッチ３のゾーニング(Zoning)設定機構３ａ、ストレージ装置４のストレージ管理機構４ａに、それぞれストージ設定、ゾーニング設定、アクセスをどこの領域に対して許可するかの設定を行う。

本発明の概要を説明する図



ンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はファイバチャネル・ネットワークを用いて複数のサーバ／複数のストレージを結合するストレージエリア・ネットワーク（以下ＳＡＮと呼ぶ）の管理システムに関する。

【０００２】

【従来の技術】近年、１台のストレージ・システムの容量が大きくなり、複数の多種多様なサーバから使用できるような機能が求められている。また、データ転送経路に高速かつ複数ホスト・ストレージ間の並列転送が可能なファイバチャネルが普及し始めたことをきっかけに、この環境での接続形体はさらに大規模化すると考えられている。このような複数のサーバ／複数のストレージ結合をストレージエリア・ネットワーク（以下ＳＡＮという）と呼び、分散化されつつある複数サーバのストレージの一元的管理やＴＯＣの削減を計ろうする試みが進みつつある。

【０００３】

【発明が解決しようとする課題】しかしながら、ストレージ内の領域管理や、セキュリティの面で解決しなければならない問題がある。その一つに、ＳＡＮが複数のホストコンピュータ（以下ホストという）及び複数のストレージ・システムより構成されていた場合に、全てのホストから全てのストレージ・システムがアクセス可能である為に、あるホストから使用しているストレージ内のデータが他のホストから不用意に破壊されてしまう可能性があった。

【０００４】ストレージ内の領域管理や、セキュリティの面で完全な対策となるものがないのが現状である。また、ＳＡＮを構成する複数装置で障害が発生した際、いろいろなエラー報告がシステム管理者に報告される為、被疑箇所を特定することが難しく方法がなかった。本発明は上記事情を考慮してなされたものであって、本発明の目的は、従来の分割されたセキュリティ方式を一元的に統合管理し、ＳＡＮにおいて最善のセキュリティ管理を自動的に行うことができるようにすることである。

【０００５】

【課題を解決するための手段】図１は本発明の概要を説明する図である。同図に示すように、本発明は上記ＳＡＮ環境に対して、ＳＡＮを統合制御する統合管理機構１を設置し、ホスト２とストレージ装置４とのアクセス関係をこの管理機構１を用いて一括して管理できるようにする。システム管理者は、統合管理機構１にホスト２側からアクセスをしようとするストレージ装置４側の領域と、そのストレージをアクセスする際の使用するファイバチャネル・アダプタ（ＦＣＡ）、ホストバス・アダプタ（ＨＢＡ）を設定する。この設定をアクセスパスと呼ぶ。設定されたアクセスパス情報を元に、この統合管理機構１は、まずホスト２側から見えるストレージ設定（Storage affinity）をホスト２側のＳＡＮ管理機構２ａに設定する。また、スイッチ３のゾーニング(Zoning)設定機構３ａに対して、ＦＣＡ，ＨＢＡが保有するＷＷＮ，ＰＩＤ情報を事前に確保しておきこれを元に設定されたアクセスパスが実現できるように計算してゾーニング(Zoning)を設定する。さらに、ストレージ装置４のストレージ管理機構４ａには、ストレージ装置のどのＦＣＡがどこのＨＢＡ（ＷＷＮ，ＰＩＤ）のアクセスをどこの領域に対して許可するかの設定を行う。上記のような統合管理機構１を設けることにより、ＳＡＮにおいて、セキュリティ管理やストレージ内の領域管理を一括して行うことができる。また、上記統合管理機構に、ＳＡＮの構成状態を構成設定情報１ａとして保持させることにより、ＳＡＮに、ＳＡＮ管理機能を持たないホストや、ゾーニング設定機能を持たないスイッチや、あるいはストレージ管理機能を持たないストレージ装置が投入されても容易に対応することができ、可能な範囲でセキュリティを確保することができる。

【０００６】さらに、上記統合管理機構１を設けることにより、以下の機能を実現することができる。

（１）統合管理機構１が、ＳＡＮの構成状態を個々の装置より確保して、構成設定情報１ａとして格納し、定期的もしくは、システム管理者からのコマンド指示によって、統合管理機構１が、現状のＳＡＮの構成状態を読込み、ＳＡＮの構成設定情報１ａと比較し、異なっていた場合は、異常と判断し、システム管理者に通知する。これにより、システム管理者はＳＡＮの異常を容易に知ることができる。

（２）統合管理機構１が、システム管理者からのコマンド指示によって、ＳＡＮ管理機構２ａ、Ｚｏｎｉｎｇ設定機構３ａ、ストレージ管理機構４ａよりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。これにより、システム管理者はアクセスパスの整合性を確認することができる。

（３）ホスト２、ホスト２のＨＢＡ、スイッチ３、あるいは、ストレージ装置３のＦＣＡが交換されたとき、上記統合管理機構１はこれを検知し、ホスト２のＳＡＮ管理機構２ａ、スイッチ３のゾーニング設定機構３ａ、もしくは、ストレージ装置４のストレージ管理機構４ａから、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定する。これにより、ＳＡＮの構成変更に対して容易に対処することができる。

（４）システム起動時にアクセスパスが設定されていな

０，４２０にはストレージ管理機構４１８，４２８を設置する。

【００１１】ＳＡＮ管理機構とは前記ａ）で説明したストレージ・アフィニティの設定を行える機構であり、ストレージ管理機構は前記したｃ）で説明したホスト・アフィニティの設定が行える機構である。さらに、スイッチ３００には前記ｂ）で説明したスイッチのゾーニング設定機構３０１が搭載される。システム管理者は、ＳＡＮ統合管理機構５００にホスト側からアクセスをしようとするストレージ側の領域と、そのストレージをアクセスする際の使用するＦＣＡ（ファイバチャネル・アダプタ），ＨＢＡ（ホストバス・アダプタ）を設定する。この設定をアクセスパスの設定と呼ぶ。設定されたアクセスパス情報は、このＳＡＮ統合管理機構５００の中で、図５（ａ）に示すＳＡＮ統合管理機構５００内アクセスパス設定情報の様に格納される。この設定情報を元に、まずホスト側から見えるストレージ設定(Storage affinity)をホスト側のＳＡＮ管理機構１１８，１２８に設定する。すなわち、どのＨＡＢからどのＦＣＡ（WWN，ＰＩＤ）へのアクセスを行うかを設定する。

【００１２】また、どのＨＢＡからどのＦＣＡに対してアクセスするかの設定は、図５（ｂ）に示すストレージ・アフィニティ（Storage Affinity）テーブルのような管理テーブルをホスト内で作成し、アクセスするＦＣＡを選択させる事で実現する。この例では、ＨＢＡ１１１からWWNｃのＦＣＡに対して領域４１５をアクセスするように設定している。ファイバチャネル上のコマンドは、相手ＦＣＡのWWNを介して発行する事が出来る。さらに、スイッチ３００のゾーニング（Zoning）設定機構３０１に対して、ＦＣＡ，ＨＢＡが保有するWWN，ＰＩＤ情報を事前に確保しておき、これを元に設定されたアクセスパスが実現できるように計算してゾーニング（Zoning）を設定する。図５（ｃ）にスイッチ・ゾーニング（Zoning）テーブルの例を示す。ここではゾーン（Zone）をＡとＢで設定し、それぞれのゾーン（Zone）に相互アクセスを許可するポート（ＨＢＡ，ＦＣＡ）の識別子（ここではWWN）を格納する。これにより、スイッチWWNａからアクセスはゾーン（Zone）Ａと認識し、WWNｃに対してのみしか実行できないようなアクセス制限を行う。

【００１３】ファイバチャネル環境ではスイッチ３００とポートを接続するとログインシーケンスが動作し、その中でスイッチはポートのWWN情報を確保できる。この情報を元に、ホスト１１０，１２０からストレージ装置４１０，４２０にコマンドが発行された場合に、ゾーン（Zone）設定されていないポートに対するアクセスが指定された時、ストレージ装置４１０，４２０のポートにコマンドが伝わらないような制御を行う。さらに、ストレージ装置４１０，４２０のストレージ管理機構４１８，４２８には、ストレージ装置４１０，４２０のどのＨＢＡ，ＰＩＤからのアクセスを、何処の領域に対して許可するかの設定を行う。図５（ｄ）にホスト・アフィニティ（Host affinity）テーブルの例を示す。このテーブルにより、ＦＣＡ４１１はWWNａのＨＢＡからのアクセスのみを領域４１５に対して許可し、ＦＣＡ４１２はWWNｅのＨＢＡからのアクセスのみを領域４１６に対して許可する。

【００１４】ファイバチャネル環境ではホストからのコマンドを受け付ける前に、ログインシーケンスという相互のポートの情報をやりとりするシーケンスがあり、その中で相手のWWNやＰＩＤなどを確認できる。ＦＣＡは、ここで確保した相手のWWNやＰＩＤの情報がアクセス許可されているものかどうかを判断し、アクセス許可がされたものに対してのみ処理を継続し、アクセス許可されていないものからのアクセスに対しては、チェックコンディション（Check condition）等でエラー応答を行う。なお、ＳＡＮを構成するホスト装置のなかにはＳＡＮ管理機構をもたない装置がある。また、ストレージ装置内でも前記c)のホスト・アフィニティ機能を提供していない装置もある。したがって、そのような装置に対して管理機構５００はアクセス関係を設定しないが、他のセキュリティ方式(Storage Affinity もしくはZoning))によってセキュリティは保護される。

【００１５】図６によりＳＡＮ統合管理機構５００が行う作業のフローチャートとその作業の具体例を説明する。まず、ＳＡＮ統合管理機構５００は、各ＦＣＡ、ＨＢＡのWWN及びＰＩＤを読み込む（ステップＳ１）。図３の例においては、ＳＡＮ統合管理機構５００が例えばホスト１１０のＨＢＡ１１１がWWNａ，ＰＩＤａであり、ストレージ装置４１０のＦＣＡ４１１がWWNｃ，ＰＩＤｃ、ＦＣＡ４１２がWWNｄ，ＰＩＤｄ等であることを認識する。ついで、ＳＡＮ統合管理機構５００は、ＨＢＡからアクセスする予定のＦＣＡと、その配下の領域を受け付ける（ステップＳ２）。図３の例においては、例えばホスト１１０のＨＢＡ１１１からストレージ装置４１０のＦＣＡ４１１経由で領域４１５にアクセスするパス設定を受け付ける。

【００１６】次に、当該ホストがストレージ・アフィニティ(Storage Affinity)機能をサポートしているかを調べる（ステップＳ３）。ストレージ・アフィニティ(StorageAffinity)機能をサポートしていない場合にはステップＳ５に行く。また、ストレージ・アフィニティ(Storage Affinity)機能をサポートしている場合にはステップＳ４において、ストレージ・アフィニティ(Storage Affinity)機能により、ＳＡＮ統合管理機構５００は、ホスト側のＳＡＮ管理機構に、ＨＢＡからアクセスできるデバイスをWWNもしくはＰＩＤを使用して設定する。例えば図３の例においては、ホスト１１０のＨＢＡ１１１から、ストレージ装置４１０のＦＣＡ４１１の識別子であるWWNｃもしくはＰＩＤｃをアクセスできるよう

ＡＮの構成設定情報５０１と比較して、異なっていた場合は、異常と判断してシステム管理者に通知する。例えば、前記図３の状態時にＳＡＮの構成設定情報５０１を登録し、その後ストレージ４２０の電源が落ちてしまった場合は、ＳＡＮの構成状態異常と判断して、システム管理者にストレージ４２０が見えなくなっていることを通知する。

【００２４】（２）アクセスパスの整合性の確認

ＳＡＮ統合管理機構５００は、システム管理者からのコマンド指示によって、ＳＡＮ管理機構１１８，１２８、ゾーニング（Zoning）設定機構３０１、ストレージ管理機構４１８，４２８よりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。この機能によりシステム管理者が勝手に個々の機器の設定を変えてしまった場合に、異常点を検出することが可能となる。また、既に、ＳＡＮがアクセスパスの設定がされた状態で存在し、新たに当該ＳＡＮ管理論理を組み込む際に、既存のＳＡＮのアクセスパスが正しく設定されているかチェックすることができる。

【００２５】（３）ＨＢＡの交換時のアクセス関係の再設定

ホスト１１０側のＨＢＡ１１１が故障して新たなＨＢＡに交換された場合、ＳＡＮ管理機構１１８はＨＢＡ交換を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、ＳＡＮ管理機構１１８はＳＡＮ統合管理機構５００に交換された新しいＨＢＡのWWNを伝える。ＳＡＮ統合管理機構５００はその新しいWWNを用いてＨＢＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング（Zoning）設定機構３０１，ストレージ管理機構４１８〕に再度アクセス関係を設定する。

【００２６】（４）ホスト交換時のアクセス関係の再設定

ホスト１１０が故障して新たなホストに交換された場合に、ホスト１１０のＳＡＮ管理機構１１８は設定がなくなっている事を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、ＳＡＮ管理機構１１８はＳＡＮ統合管理機構５００に接続されているＨＢＡのWWNを伝え、ＳＡＮ統合管理機構５００は、そのWWNを用いてＨＢＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング（Zoning）設定機構３０１，ストレージ管理機構４１８〕に再度アクセス関係を設定する。

【００２７】（５）スイッチ交換時のアクセス関係の再設定

スイッチ３００が故障して交換された際に、スイッチに設定したゾーニング（Zoning）情報がなくなっている事を検出し、システム管理者に通知する。ＳＡＮ統合管理機構５００に、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせる機構を設け、このような場合に、ＳＡＮ統合管理機構５００から、新しいスイッチに故障前のアクセス関係を再設定する。なお、スイッチ３００が故障して交換された際に、スイッチに設定したゾーニング（Zoning）情報がなくなっている事を検出するが、システム管理者には通知せず、自動的にＳＡＮ統合管理機構５００から新しいスイッチに故障前のアクセス関係をセットさせる機構をＳＡＮ統合管理機構５００に設け、再設定できるようにしてもよい。

【００２８】（６）ＦＣＡ交換時のアクセス関係の再設定

ストレージ装置側４１０のＦＣＡ４１１が故障し交換され、ＦＣＡ側のWWNが変更されてしまった場合に、これを検出しシステム管理者に通知する。システム管理者からの構成再設定コマンドによって、ストレージ管理機構４１８が新しいＦＣＡのWWNを検出してＳＡＮ統合管理機構５００に伝え、ＳＡＮ統合管理機構５００はその新しいWWNを用いてＦＣＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ＳＡＮ管理機構１１８、ゾーニング（Zonig)設定機構３０１〕に再度アクセス関係を設定する。

【００２９】（７）不用意なアクセスの設定の防止

前述したように、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐ為に、システム起動時にアクセスパスが設定されていない状態時に、スイッチに対して全てのアクセスを許可しない設定を行う。このような設定がないと、全てのＳＡＮのストレージに対して全てのホストからアクセス出来てしまい、セキュリティ上の問題が生ずることがある。

（８）ファイバチャネルの転送クラスの設定

ファイバチャネル（ＦＣ）ではＨＢＡとＦＣＡ側で共通に設定すべきＦＣの転送クラス（Ｃｌａｓｓ）というパラメータがある。転送クラスにはクラス１～３があり、転送クラス１は殆ど使用されず、転送クラス２は転送後、アクノリッジを返し、転送クラス３は転送後、アクノリッジを返さない転送方式である。このパラメータがＨＢＡＩ側とＦＣＡ側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用するＣｌａｓｓもシステム管理者に指定させて、管理機構５００がＳＡＮ管理機構１１８，１２８、ストレージ管理機構４１８，４２８を通じて、アクセスパスを設定したＨＢＡとＦＣＡが指定された同一のＣｌａｓｓで動作させるようにする。

【００３０】次に、上記ＳＡＮ統合管理機構５００を用いたＳＡＮの障害監視について説明する。基本的にＳＡＮ統合管理機構５００を用いた場合は、ＳＡＮを構成する装置（ホスト、スイッチ、ストレージ装置）で発生し

もに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

（付記２）上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報として保持し、定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報と集収した現状の構成情報とを比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする付記１のストレージエリア・ネットワーク管理システム。

（付記３）上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および／またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする付記１または付記２のストレージエリア・ネットワーク管理システム。

（付記４）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ホストコンピュータ、ホストコンピュータに設けられたホストバス・アダプタ、スイッチ、あるいは、ストレージ装置に設けられたファイバチャネル・アダプタが交換されたとき、上記統合管理機構はこれを検知し、上記ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチの領域設定機構、もしくは、ストレージ装置のストレージ管理機構から、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定することを特徴とするストレージエリア・ネットワーク・システム。

（付記５）ホストコンピュータのホストバス・アダプタが故障して交換された際、統合管理機構はホストバス・アダプタの交換を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、統合管理機構１は、ホストコンピュータのストレージエリア・ネットワーク管理機構に交換された新しいホストバス・アダプタの設定情報を伝え、該新しい設定情報を用いてホストバス・アダプタ交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記６）ホストコンピュータが故障して交換された際、統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構の設定がなくなっている事を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、上記ストレージエリア・ネットワーク管理機構は統合管理機構に対して接続されているホストバス・アダプタの設定情報を伝え、統合管理機構はその情報を用いてホストコンピュータ交換前と同等のアクセス関係を構築し、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記７）スイッチが故障して交換された際、統合管理機構は、スイッチに設定した領域設定情報がなくなっている事を検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記８）スイッチが故障して交換された際に、スイッチに設定した領域設定情報がなくなっている事を検出し、統合管理機構は、自動的に新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記９）ストレージ装置側のファイバチャネル・アダプタ交換され、ファイバチャネル・アダプタの設定情報が変更された場合、統合管理機構は、これを検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、ストレージ管理機構が新しい設定情報を統合管理機構に伝え、統合管理機構はその新しい設定情報を用いて交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記１０）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレー

タのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

（付記１９）複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

（付記２０）複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【００３８】

【発明の効果】以上説明したように、本発明においては、ＳＡＮにストレージエリア・ネットワークを統合制御する統合管理機構を設け、ホストとストレージとのアクセス関係を上記統合管理機構により一括して管理するようにしたので、以下の効果を得ることができる。

（１）信頼性の高い一元管理されたＳＡＮシステムを構築することができる。また、前記したホスト・アフィニティ、ゾーニング等の機能を持っていない、過去のシステムに対しても対応できるので、全て新しいシステムを購入してＳＡＮを構築することが動作環境の必須条件とならない。

（２）ＳＡＮの異常や、アクセスパスの整合性を容易に確認することができる。

（３）ＳＡＮを構成するホスト、ＨＡＢ、スイッチ、ストレージ装置、ＦＣＡ等が交換され、ＳＡＮの構成状態が変更されても容易に対応することができる。

（４）ＳＡＮに異常が発生した場合、被疑箇所やその影響範囲を容易に特定することができ、業務影響を最小限に止めることができる。

【図面の簡単な説明】

【図１】本発明の概要を説明する図である。

【図２】本発明の対象となるＳＡＮシステムの構成例を示す図である。

【図３】本発明の実施例のＳＡＮ管理システムの構成を示す図である。

【図４】ストレージ装置のハードウェア構成例を示す図である。

【図５】アクセスパス設定情報、ストレージ・アフィニティ・テーブル、スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブルの例を示す図である。

【図６】ＳＡＮ統合管理機構が行う処理のフローチャートを示す図である。

【図７】ゾーニング設定機構が行う処理のフローチャートを示す図である。

【図８】ＳＡＮの障害管理を説明する図である。

【図９】障害報告方法定義の一例を示す図である。

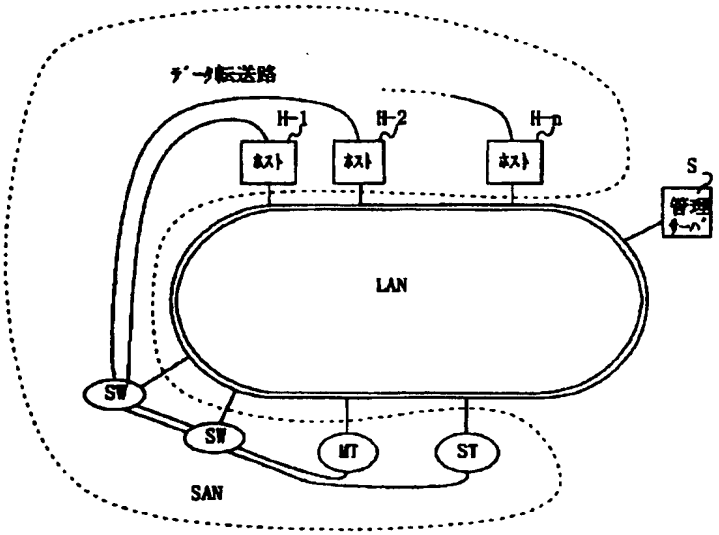
【図１０】ＳＡＮ統合管理機構が行うＳＡＮの障害監視機能のフローチャートである。

【符号の説明】

１	統合管理機構
１ａ	構成設定情報
２	ホスト
２ａ	ＳＡＮ管理機構
３	スイッチ
３ａ	ゾーニング(Zoning)設定機構
４	ストレージ装置
４ａ	ストレージ管理機構
１１０，１２０	ホスト
１１１，１１２	ホストバス・アダプタ（ＨＢＡ）
１２１	ホストバス・アダプタ（ＨＢＡ）
３００	スイッチ
３０１	ゾーニング設定情報
４１０，４２０	ストレージ装置
４１１，４２１	ファイバチャネル・アダプタ（ＦＣＡ）
４２１	ファイバチャネル・アダプタ（ＦＣＡ）
４１８，４２８	ストレージ管理機構
５００	ＳＡＮ統合管理機構
５０１	ＳＡＮ構成設定情報

【図２】

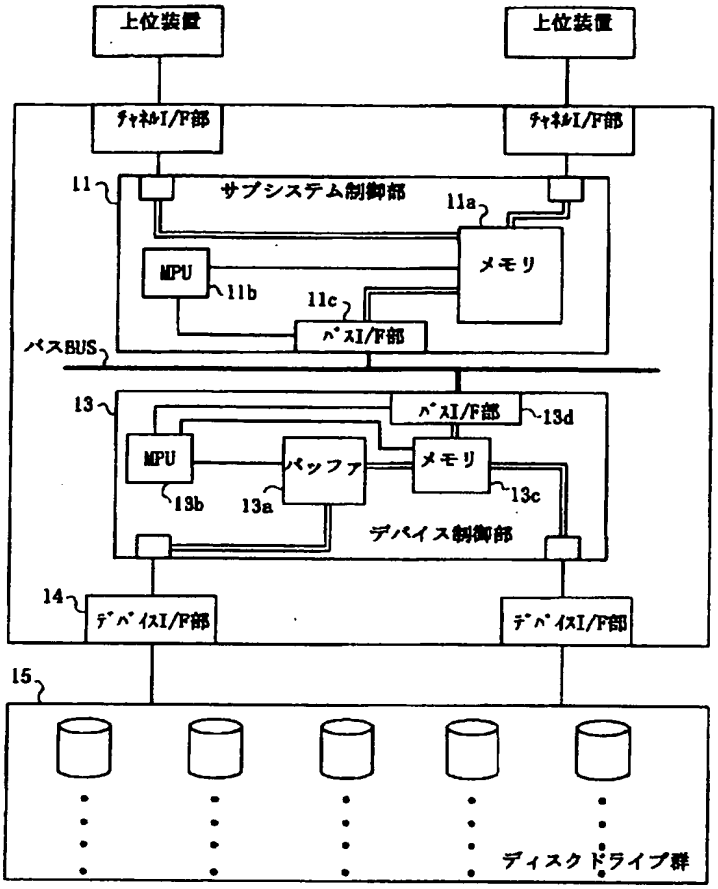
本発明の対象となるＳＡＮシステムの構成例を示す図



ST:ストレージ装置
MT:磁気テープ装置
SW:スイッチ

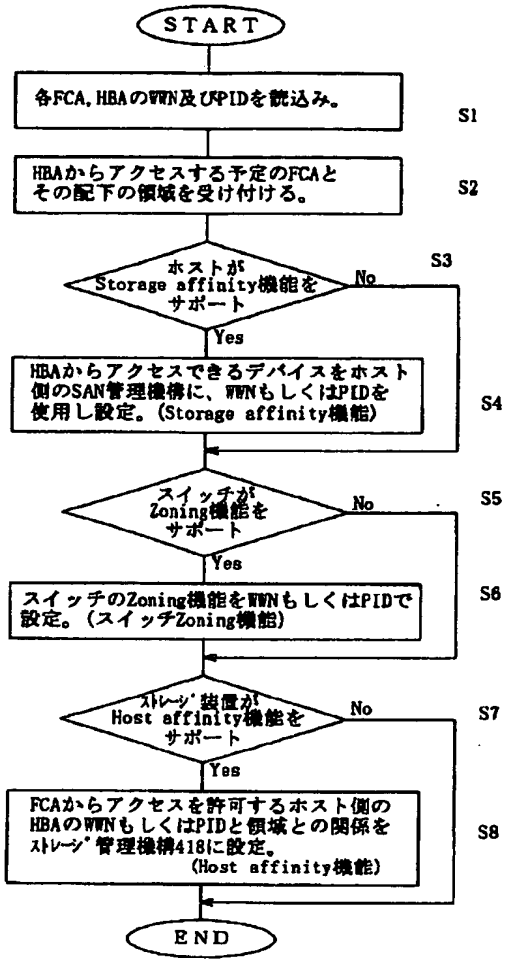
【図４】

本発明の実施例のストレージ装置のハードウェア構成例を示す図



【図６】

ＳＡＮ統合管理機構が行う処理のフローチャートを示す図



【図８】

ＳＡＮの障害管理を説明する図